IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

JOHN DOE (an alias), individually and on behalf of all others similarly situated,	)	
Plaintiff,	)	Case No.
v.	)	
AVID LIFE MEDIA, INC., an Ontario corporation and AVID DATING LIFE, INC., an Ontario corporation d/b/a ASHLEY MADISON,	)	**JURY TRIAL DEMANDED**
Defendants.	)	

CLASS ACTION COMPLAINT

Plaintiff John Doe ("Plaintiff") brings this Class Action Complaint against Defendants Avid Life Media, Inc. and Avid Dating Life, Inc., d/b/a Ashley Madison ("Defendants" or "Ashley Madison"), individually and on behalf of all others similarly situated, and complains and alleges upon personal knowledge as to himself and his own acts and experiences and, as to all other matters, upon information and belief, including investigation conducted by his attorneys.

I. NATURE OF THE ACTION

1. Defendants operate a dating site, ashleymadison.com, which is designed to facilitate intimate adult relationships for individuals who are either married or are in committed relationships. The website currently has over 39 million "anonymous" users. According to the site:

> Ashley Madison is the most famous name in infidelity and married dating. As seen on Hannity, Howard Stern, TIME, BusinessWeek, Sports Illustrated, Maxim, USA Today. Ashley Madison is the most recognized and reputable married dating company. Our Married Dating Services for Married individuals Work. Ashley Madison is the most successful website for finding an affair and cheating partners.

> Have an Affair today on Ashley Madison. Thousands of cheating wives and cheating husbands signup everyday looking for an affair. We are the most famous website for discreet encounters between married individuals. Married Dating has never been easier. With Our affair guarantee package we guarantee you will find the perfect affair partner. Sign up for Free today.

2. Because of the nature of the site, Ashley Madison stores highly personal and private information of its customers along with financial information. This information includes login information, mailing addresses, email addresses, phone numbers, payment transaction details, credit and debit card data, as well as passwords and information on how much each user spent on Ashley Madison services. Unlike other commercial websites, however, each user of Ashley Madison creates a profile on the site, which includes highly personal information, including photographs and sexual fantasies of the user. One of the primary purposes of Ashley Madison is to maintain users' confidentiality and anonymity.

3. On or about July 15, 2015, Defendants' website experienced a massive data breach (the "Security Breach") exposing highly personal and financial information of 37 million ashleymadison.com users. Following this theft of information, the hackers (known as "Impact Team") threatened to release all customer information on the Internet if Defendants did not shut down the site.

4. On or about August 18, 2015, Impact Team released 9.7 gigabytes worth of stolen and highly-sensitive personal and financial data including the information of Plaintiff and Class Members. Reportedly, among the disseminated data was the data of people who specifically paid Defendants a $19 fee to have their profiles deleted from the site.

5. On or about August 20, 2015, even more personal information of Ashley Madison users was similarly released. Despite being told that it could prevent the release of personal information of Plaintiff and Class Members, Ashley Madison allowed such personal information

to be released and did not notify Plaintiff and Class Members about the threat of the release of personal information or the actual release of personal information.

6. Defendants' security failures enabled the hackers to steal this information and otherwise put Class members' information at serious and ongoing risk. The hackers continue to use the information they obtained as a result of Defendants' inadequate security to exploit and injure Plaintiff and Class members across the United States.

7. The Security Breach was caused and enabled by Defendants' knowing violation of its obligations to abide by best practices and industry standards in protecting its customers' personal information. Defendants grossly failed to comply with security standards and allowed its customers' financial information to be compromised, all in an effort to save money by cutting corners on security measures that could have prevented or mitigated the Security Breach that occurred.

8. Indeed, upon information and belief, in an internal company file called "Areas of concern – customer data.docx," an unnamed Ashley Madison employee lists technical issues that could lead to a data breach, as well the legal problems likely to ensue. Under a section called "Data leak/threft issues [sic]," the author lists customer data being exposed by phishing or SQL injection being a possible problem when malicious requests are punched into an entry field, typically in order to dump the site database. Another Ashley Madison employee worried about remote code execution—when an attacker can run code on a victim's computer over the internet—and yet another employee pointed to employees being infected with malware, "allowing hackers access to our user data."

9. In the aftermath of the Security Breach, Defendants failed to uncover and disclose the extent of the Security Breach and notify affected customers of the Breach in a timely manner.

Defendants failed to take other reasonable steps to clearly and conspicuously inform customers of the nature and extent of the Security Breach. Furthermore, by failing to provide adequate notice, Defendants prevented Class members from protecting themselves from the Security Breach and caused Plaintiff and Class Members to suffer financial loss, emotional distress and disastrous consequences given the nature of the information.

10. Accordingly, Plaintiff, on behalf of himself and other members of the Class, asserts claims for breach of express and implied contract, violations of the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq*., bailment, unjust enrichment and seeks injunctive relief, declaratory relief, monetary damages, statutory damages, and all other relief as authorized in equity or by law.

II. JURISDICTION AND VENUE

11. This Court has original jurisdiction pursuant to 28 U.S.C. § 1332(d)(2). In the aggregate, Plaintiff's claims and the claims of the other members of the Class exceed $5,000,000 exclusive of interest and costs, and there are numerous class members who are citizens of States other than Defendants' state of citizenship.

12. This Court has personal jurisdiction over Defendants because Defendants: (a) intentionally avail themselves of this jurisdiction by marketing their website to millions of consumers nationwide, including residents of Illinois and this District; and (b) have directed tortious acts toward individuals residing within this District, and have committed tortious acts that they know or should have known would cause injury to Plaintiff and Class Members in this District.

13. Venue is proper within this District under 28 U.S.C. § 1391(b)-(c) because: (a) Defendants regularly transact business within this District; (b) certain acts giving rise to the

claims asserted in this Complaint occurred in this District; and (c) the actions of Defendants alleged in this Complaint caused damages to Plaintiff and a substantial number of Class Members within this District.

III. PARTIES

Plaintiff

14. Plaintiff is citizen of the State of Illinois and is domiciled in Cook County, Illinois. Upon information and belief, Plaintiff created an account with Ashley Madison in May of 2015 with a heightened expectation of privacy due to the nature of Defendants' services. As part of the process of creating his account, Plaintiff created a username and password and entered his personal information into the website, including photographs. Plaintiff subsequently purchased credits and communicated with other members on the website. In signing up with the site and subsequently paying to use it, Plaintiff contracted with Ashley Madison for the adequate protection of his sensitive personal and financial information. As a result of Ashley Madison's inadequate security, Plaintiff's personal information was exposed.

Ashley Madison

15. Defendant Avid Life Media, Inc. is a Canadian corporation organized and existing under the laws of Ontario, Canada, with its principal place of business and headquarters in Toronto, Canada. The corporation owns various companies that are in business of operating online dating websites.

16. Defendant Avid Dating Life, Inc. d/b/a Ashley Madison is a corporation organized and existing under the laws of Ontario, Canada, with its principal place of business in Toronto, Canada, and is regularly engaged in the business of operating online dating websites, including ashleymadison.com.

IV. FACTUAL BACKGROUND

The Data Breach

17. The site ashleymadison.com is a dating website marketed to people seeking to engage in adulterous behavior. Because of the nature of the site, Ashley Madison makes numerous representations to its customers that it will keep their information secure and private and that their information "will never be shown or shared." To provide extra protection to customers, the website even offers to "scrub" – or delete – user profiles along with all personal information for a $19 charge.

18. Defendants market ashleymadison.com all over the world. The website currently has more than 39 million users. It is rated the twentieth most popular adult website in the United States. Defendants market the website through television, radio, billboard, and internet advertisements, many of which include its founder and CEO Noel Biderman as the website's spokesperson.

19. The website's business model is based on credits, which users purchase, as opposed to paid subscriptions. In order to contact another user, one must "pay" five credits. Users buy credits from the website and enter their credit or debit card information in order to pay for the credits.

20. In order to create an account, users are required to select a username and password, personalize a "greeting," indicate their location (by country), zip code, date of birth, type of affair sought – the options provided are short term, long term, cyber affair/erotic chat, or other – height, weight, body type, ethnicity and email. The website asks users to upload a "discrete photo" which the site can alter by inserting a mask over the user's eyes or else blur the

photo. The user can also enter information concerning "My Intimate Desires," "My Perfect Match," and "My Personal Interests," among other things.

21. Upon information and belief, Ashley Madison stores this information in an unencrypted format, making it highly vulnerable and susceptible to security breaches. Defendants should have known of security threats yet, despite this, Defendants insisted on representing that the Ashley Madison site as "the last truly secure space on the Internet."

22. Those representations proved false. As a result of Defendants' failure to maintain adequate and reasonable security measures to secure the data of their customers, on or about July 15, 2015, a group of hackers known as "Impact Team" downloaded highly-sensitive personal, financial, and identifying information of nearly 40 million of the website's users. On information and belief, among the data compromised and downloaded were profiles of individuals who executed a "paid delete" option to scrub their user profiles and all associated data and paid $19 to Defendants to do so, yet Defendants failed to actually scrub the data.

23. Following the Security Breach and downloading of users' personal and financial information, Impact Team threatened in an online manifesto on July 15, 2015 that, if Defendants did not shut down the website permanently, they would leak the information on the Internet.

24. Defendants confirmed on July 20, 2015 that the personal information of nearly 40 million members worldwide was accessed by the hackers, but they refused to take down the site. On or about August 18, 2015, Impact Team, in keeping with its threat, published 9.7 gigabytes of stolen personal information of the website users on the Internet, including the personal information of Plaintiff and Class Members. On or about August 20, 2015, additional personal information of Plaintiff and Class Members was similarly released. Despite being told by the hackers that they could have prevented the release of the personal information of Plaintiff and

Class Members, Defendants allowed such personal information to be released to the public and did not notify Plaintiff and Class Members about the threat of the release of or the actual release of the personal information.

25. This massive data breach could have been prevented in the first place had Defendants taken the necessary and reasonable precautions to protect their users' information by, for example, encrypting the data entrusted to them by users. Defendants were aware or should have been aware of the need to secure users' information, especially in light of the recent rise in massive security breaches on the Internet and the fact that the information contained on Defendants' servers is particularly sensitive.

26. Upon information and belief, in an internal company file called "Areas of concern – customer data.docx," an unnamed Ashley Madison employee identified technical issues that could lead to a data breach, as well as legal problems likely to ensue. Under a section called "Data leak/threft issues [sic]," the author listed customer data being exposed by phishing or SQL injection as a possible problem when malicious requests are punched into an entry field, typically in order to dump the site database. Another Ashley Madison employee worried about remote code execution—when an attacker can run code on a victim's computer over the internet—and yet another employee pointed to employees being infected with malware, "allowing hackers access to our user data."

27. Defendants' lax security allowed private user information and personal financial information connected with millions of customer credit cards and debit cards, including credit cards and debit cards of Plaintiff and Class Members to become compromised for a period prior to July 15, 2015.

28. Even after becoming aware on July 15, 2015 of the Security Breach, Ashley Madison failed to notify Plaintiff and Class Members of the breach in a timely manner after learning of the breach and failed to take reasonable steps to inform Plaintiff and Class Members of the extent of the breach.

29. As a result of Defendants' unfair, unreasonable, and inadequate data security, its users' extremely personal and embarrassing information is now accessible to the public. In addition to the embarrassing information regarding users' sexual interests or the fact that users were seeking or had affairs, users' addresses, phone numbers, email addresses, credit card or other payment information, birth dates, and photos are also now available on the Internet. For many of the website's users, the publicity of this information has created and will continue to create irreparable harm.

30. Defendants' failure to comply with reasonable security standards provided short-term and fleeting benefits in the form of saving on the costs of compliance, but at the expense and to the severe detriment of its own customers – including Class members here – who have been subject to the Security Breach or otherwise have had their highly sensitive personal and financial information placed at serious and ongoing risk.

31. Defendants allowed widespread and systematic theft of their customers' financial information and potentially embarrassing personal information. Defendants' actions did not come close to meeting the standards of commercially reasonable steps that should be taken to protect such intensely personal information.

Damages Sustained By Plaintiff and the Class

32. Plaintiff and Class Members are subject to continuing damage from having their Personal Information comprised as a result of Defendants' inadequate systems and failures. Such

damages include, among other things, the amount paid to Defendants to allow them to anonymously contact members on the site; the amount paid to Defendants to perform a "paid-delete" which Defendants did not perform or performed inadequately; out-of-pocket expenses incurred to mitigate the increased risk of identity theft and or fraud; credit, debit, and financial monitoring to prevent and/or mitigate theft, identity theft, and/or fraud incurred or likely to occur as a result of Defendants' security failures; the value of their time and resources spent mitigating the identity theft and/or fraud; the cost of and time spent replacing credit cards and debit cards and reconfiguring automatic payment programs with other merchants related to the compromised cards; and irrecoverable financial losses due to unauthorized charges on the credit/debit cards of Defendants' customers by identity thieves who wrongfully gained access to the Personal Information of Plaintiff and the Classes, the embarrassment of having Personal Information disclosed, the damage to marital relationships due to the breach, and the emotional distress of such breach. Plaintiff has sustained these injuries and is in immediate danger of sustaining further direct injuries as the result of Defendants' actions and inactions. To date, Ashley Madison has not offered any form of credit monitoring or identity theft protection services to any of its affected customers.

V. CLASS ACTION ALLEGATIONS

33. Plaintiff brings Counts I, II, V and VI as set forth below, on behalf of himself and as a class action, pursuant to the provisions of Rule 23 of the Federal Rule of Civil Procedure on behalf of a class defined as:

> All citizens of the United States who were users of www.ashleymadison.com and had their information compromised in the Security Breach (the "National Class").

Excluded from the National Class are Defendants and their affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded are any judicial officers presiding over this matter and the members of their immediate families and judicial staff.

34. Plaintiff brings Count III, as set forth below, on behalf of himself and as a class action, pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure on behalf of a class defined as:

> All citizens of the Consumer Fraud States[1] who were users of www.ashleymadison.com and had their information compromised in the Security Breach (the "Consumer Fraud Multistate Class").

Excluded from the Consumer Fraud Multistate Class are Defendants and their affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded are any judicial officers presiding over this matter and the members of their immediate families and judicial staff.

35. In the alternative to Count III, Plaintiff brings Count IV, as set forth below, on behalf of himself and as a class action, pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure on behalf of the following state sub-class, defined as:

> All citizens of the State of Illinois who were users of www.ashleymadison.com and had their information compromised in the Security Breach (the "Illinois State Class").

[1] The States that have similar consumer fraud laws based on the facts of this case are: Arkansas (Ark. Code § 4-88-101, *et seq.*); California (Cal. Bus. & Prof. Code §17200, *et seq.* and Cal. Civil Code § 1750, *et seq.*); Colorado (Colo. Rev. Stat. § 6-1-101, *et seq.*); Connecticut (Conn. Gen. Stat. § 42-110, *et seq.*); Delaware (Del. Code tit. 6, § 2511, *et seq.*); District of Columbia (D.C. Code § 28-3901, *et seq.*); Florida (Fla. Stat. § 501.201, *et seq.*); Hawaii (Haw. Rev. Stat. § 480-1, *et seq.*); Idaho (Idaho Code § 48-601, *et seq.*); Illinois (815 ICLS § 505/1, *et seq.*); Maine (Me. Rev. Stat. tit. 5 § 205-A, *et seq.*); Massachusetts (Mass. Gen. Laws Ch. 93A, *et seq.*); Michigan (Mich. Comp. Laws § 445.901, *et seq.*); Minnesota (Minn. Stat. § 325F.67, *et seq.*); Missouri (Mo. Rev. Stat. § 407.010, *et seq.*); Montana (Mo. Code. § 30-14-101, *et seq.*); Nebraska (Neb. Rev. Stat. § 59-1601, *et seq.*); Nevada (Nev. Rev. Stat. § 598.0915, *et seq.*); New Hampshire (N.H. Rev. Stat. § 358-A:1, *et seq.*); New Jersey (N.J. Stat. § 56:8-1, *et seq.*); New Mexico (N.M. Stat. § 57-12-1, *et seq.*); New York (N.Y. Gen. Bus. Law § 349, *et seq.*); North Dakota (N.D. Cent. Code § 51-15-01, *et seq.*); Oklahoma (Okla. Stat. tit. 15, § 751, *et seq.*); Oregon (Or. Rev. Stat. § 646.605, *et seq.*); Pennsylvania (73 P.S. § 201-1, *et seq.*); Rhode Island (R.I. Gen. Laws § 6-13.1-1, *et seq.*); South Dakota (S.D. Code Laws § 37-24-1, *et seq.*); Virginia (VA Code § 59.1-196, *et seq.*); Vermont (Vt. Stat. tit. 9, § 2451, *et seq.*); Washington (Wash. Rev. Code § 19.86.010, *et seq.*); West Virginia (W. Va. Code § 46A-6- 101, *et seq.*); and Wisconsin (Wis. Stat. § 100.18, *et seq.*).

Excluded from the Illinois State Class are Defendants and their affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded are any judicial officers presiding over this matter and the members of their immediate families and judicial staff.

36. The National Class, Consumer Fraud Multistate Class, and Illinois State Class are collectively referred to as the "Class," unless specifically indicated otherwise.

37. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of his claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

38. **Numerosity – Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous that their individual joinder herein is impracticable. On information and belief, Class members number in the thousands to millions. The precise number of Class members and their addresses are presently unknown to Plaintiff, but may be ascertained from Defendant's books and records. Class members may be notified of the pendency of this action by mail, email, Internet postings, and/or publication.

39. **Commonality and Predominance – Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** Common questions of law and fact exist as to all Class members and predominate over questions affecting only individual Class members. Such common questions of law or fact include:

a. Whether Defendants failed to use reasonable care and commercially reasonable methods to secure and safeguard their customers' sensitive personal and financial information;

b. Whether Defendants properly implemented any security measures to protect customer personal and financial information from unauthorized capture, dissemination, and misuse;

c. Whether Defendants' conduct violates the Illinois and other asserted Consumer Fraud Acts;

d. Whether Defendants' conduct constitutes breach of an implied contract; and

e. Whether Plaintiff and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief.

40. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff on behalf of himself and the other Class members. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action.

41. **Typicality – Federal Rule of Civil Procedure 23(a)(3).** Plaintiff's claims are typical of the claims of the other Class members because, among other things, all Class members were comparably injured through Defendants' uniform misconduct described above and were thus all subject to the Security Breach alleged herein. Further, there are no defenses available to Defendants that are unique to Plaintiff.

42. **Adequacy of Representation – Federal Rule of Civil Procedure 23(a)(4).** Plaintiff is an adequate Class representative because his interests do not conflict with the interests of the other Class members he seeks to represent, he has retained counsel competent and experienced in complex class action litigation, and he will prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiff and his counsel.

43. **Insufficiency of Separate Actions – Federal Rule of Civil Procedure 23(b)(1).** Absent a representative class action, members of the Class would continue to suffer the harm described herein, for which they would have no remedy. Even if separate actions could be brought by individual consumers, the resulting multiplicity of lawsuits would cause undue hardship and expense for both the Court and the litigants, as well as create a risk of inconsistent rulings and adjudications that might be dispositive of the interests of similarly situated purchasers, substantially impeding their ability to protect their interests, while establishing incompatible standards of conduct for Defendants. The proposed Class thus satisfies the requirements of Fed. R. Civ. P. 23(b)(1).

44. **Declaratory and Injunctive Relief – Federal Rule of Civil Procedure 23(b)(2).** Defendants have acted or refused to act on grounds generally applicable to Plaintiff and the other Class members, thereby making appropriate final injunctive relief and declaratory relief, as described below, with respect to the members of the Class as a whole.

45. **Superiority – Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and the other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be impracticable for Class members to individually seek redress for Defendants' wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties

and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

VI. CLAIMS ALLEGED

COUNT I
Breach of Express Contract
(On Behalf of Plaintiff and the National Class)

46. Plaintiff incorporates paragraphs 1-32 as if fully set forth herein.

47. When Plaintiff and Class members provided their personal and financial information to ashleymadison.com in order to receive the website's services, they entered into express contracts with Defendants pursuant to which Defendants agreed to safeguard and protect such information from being compromised.

48. Defendants solicited Plaintiff and Class members to sign up with ashleymadison.com and to provide their personal and financial information. Plaintiff and Class members later paid fees to Defendants based on Defendants' express representations concerning the safeguarding and protection of personal information.

49. Plaintiff and Class members fully performed their obligations under the contracts with Defendants.

50. Defendants breached the contracts and did not safeguard or protect Plaintiff's and the proposed Class members' personal data from being accessed, compromised, and/or stolen. Defendants did not maintain sufficient security measures and procedures to prevent unauthorized access to Plaintiff's and the Class members' personal and financial information.

51. Plaintiff and Class members had their personal and financial information stolen as a result of the Security Breach.

52. Plaintiff and the Class members have suffered and will continue to suffer damages as the result of Defendants' breach, including the monetary fees that Plaintiff and Class members paid to Ashley Madison.

53. The losses and damages sustained by Plaintiff and Class members as described herein were the direct and proximate result of Defendants' breaches of the contracts between them and Plaintiff and Class Members.

COUNT II
Breach of Implied Contract
(On Behalf of Plaintiff and the National Class)

54. Plaintiff incorporates paragraphs 1-32 as if fully set forth herein.

55. When Plaintiff and Class members provided their personal and financial information to ashleymadison.com in order to receive the website's services, they entered into implied contracts with Defendants pursuant to which Defendants agreed to safeguard and protect such information from being compromised.

56. Defendants solicited Plaintiff and Class members to sign up with ashleymadison.com and to provide their personal and financial information. Plaintiff and Class Members accepted the website's offer and provided their personal information in order to sign up and later their financial information in order to purchase credits. Plaintiff and Class members paid this money to Defendants in exchange for Defendants' promise to protect their anonymity and confidentiality.

57. Plaintiff and Class members would not have provided and entrusted their financial and personal information to Defendants in the absence of the implied contracts.

58. Plaintiff and Class members fully performed their obligations under the implied contracts with Defendants.

59. In the contracts, Defendants promised to safeguard and protect Plaintiff's and

Class members' private personal and financial information from being compromised and/or stolen.

60. Plaintiff and class members fully performed their obligations under the implied contracts.

61. Defendants breached the implied contracts and did not safeguard or protect Plaintiff's and the proposed Class members' personal data from being accessed, compromised, and/or stolen. Defendants did not maintain sufficient security measures and procedures to prevent unauthorized access to Plaintiff's and the Class members' personal and financial information.

62. Defendants' failure to fulfill their implied contractual obligations resulted in Plaintiff and the Class members receiving services of far less value than what was promised, i.e., services that included adequate protection of confidential information. Accordingly, Plaintiff and the Class members did not receive the full benefit of their bargain.

63. Plaintiff and the Class members have suffered and will continue to suffer damages as the result of Defendants' breach, including the monetary difference between the amount paid for services as promised (which were promised to include adequate data protection) and the services actually provided by Defendants (which did not include adequate data protection).

64. The losses and damages sustained by Plaintiff and Class members as described herein were the direct and proximate result of Defendants' breaches of the implied contracts between them and Plaintiff and Class Members.

COUNT III
Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act (and Substantially Similar Laws of the Consumer Fraud States) (on Behalf of the Consumer Fraud Multistate Class)

65. Plaintiff incorporates paragraphs 1-32 as if fully set forth herein.

66. Plaintiff and the other members of the Class were deceived by Defendants' failure to properly implement adequate, commercially reasonable security measures to protect their private personal and financial information.

67. Defendants intended for Plaintiff and the other members of the Class to rely on them that the information furnished to Defendants would be protected, secure, and not susceptible to access from unauthorized third parties.

68. Defendants instead mishandled Plaintiff's and the other Class members' personal information in such manner that it was compromised.

69. Defendants failed to follow industry best practices concerning data theft or were negligent in preventing such data theft from occurring.

70. It was foreseeable that Defendants' willful indifference or negligent course of conduct in handling their customers' personal information would put that information at risk of compromise by data thieves.

71. Defendants benefited from mishandling customers' personal information because, by not taking preventative measures that would have prevented the data from being compromised, Defendants saved on the cost of those security measures.

72. Defendants' fraudulent and deceptive acts and omissions were intended to induce Plaintiff's and the other Class members' reliance on Defendants' deception that their personal and financial information was secure and protected.

73. Defendants violated 815 ILCS 505/2 by failing to properly implement adequate, commercially reasonable security measures to protect Plaintiff's and the other Class members' private personal and financial information, by failing to warn them that their information was at risk, and by failing to discover and immediately notify affected customers of the nature and extent of the Security Breach.

74. Defendants' acts or practice of failing to employ reasonable and appropriate security measures to protect consumers' personal information constitute violations of the Federal Trade Commission Act, 15 U.S.C. § 45(a).

75. Defendants' conduct constitutes unfair acts or practices as defined in that statute because Defendants caused substantial injury to Class members that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers.

76. In addition, Defendants also engaged in an unlawful practice by failing to comply with 815 ILCS 530/10(a), which provides:

> Sec. 10. Notice of Breach. (a) Any data collector that owns or licenses personal information concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach. The disclosure notification shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system

77. 815 ILCS 530/20 provides that a violation of 815 ILCS 530/10 "constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act."

78. Plaintiff and the other members have suffered injury in fact and actual damages including lost money and property as a result of Defendants' violations of 815 ILCS 505/2.

79. Plaintiff's and the other Class members' injuries were proximately caused by Defendants' fraudulent and deceptive behavior, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is appropriate.

80. By this conduct, Defendants violated the substantive consumer protection and unfair deceptive trade practices acts or statutes of the Consumer Fraud States, whose laws do not materially differ from that of Illinois, or conflict with each other for purposes of this action.

COUNT IV
Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act (In the alternative to Count III and on Behalf of the Illinois State Class)

81. Plaintiff incorporates paragraphs 1-32 as if fully set forth herein.

82. Plaintiff and the other members of the Class were deceived by Defendants' failure to properly implement adequate, commercially reasonable security measures to protect their private personal and financial information.

83. Defendants intended for Plaintiff and the other members of the Class to rely on Defendants to protect the information furnished to them in such manner that the transactions would be protected, secure, and not susceptible to access from unauthorized third parties.

84. Defendants instead mishandled Plaintiff's and the other Class members' personal information in such manner that it was compromised.

85. Defendants failed to follow industry best practices concerning data theft or were negligent in preventing such data theft from occurring.

86. It was foreseeable that Defendants' willful indifference or negligent course of conduct in handling their customers' personal information would put that information at risk of compromise by data thieves.

87. Defendants benefited from mishandling their customers' personal information because, by not taking preventative measures that would have prevented the data from being compromised, Defendants saved on the cost of those security measures.

88. Defendants' fraudulent and deceptive acts and omissions were intended to induce Plaintiff's and the other Class members' reliance on Defendants' deception that their financial information was secure and protected.

89. Defendants violated 815 ILCS 505/2 by failing to properly implement adequate, commercially reasonable security measures to protect Plaintiff's and the other Class members' private financial information, by failing to warn users that their information was at risk, and by failing to discover and immediately notify affected customers of the nature and extent of the security breach.

90. Defendants' acts or practice of failing to employ reasonable and appropriate security measures to protect consumers' personal information constitute violations of the Federal Trade Commission Act, 15 U.S.C. § 45(a).

91. Defendants' conduct constitutes unfair acts or practices as defined in that statute because Defendants caused substantial injury to Class members that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers.

92. In addition, Defendants also engaged in an unlawful practice by failing to comply with 815 ILCS 530/10(a), which provides:

> Sec. 10. Notice of Breach. (a) Any data collector that owns or licenses personal information concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach. The disclosure notification shall be made in the most expedient time possible and without unreasonable delay, consistent

> with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system

93. 815 ILCS 530/20 provides that a violation of 815 ILCS 530/10 "constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act."

94. Plaintiff and the other Class members have suffered injury in fact and actual damages including lost money and property as a result of Defendants' violations of 815 ILCS 505/2.

95. Plaintiff's and the other Class members' injuries were proximately caused by Defendants' fraudulent and deceptive behavior, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is appropriate.

COUNT V
Bailment
(On Behalf of Plaintiff and the National Class)

96. Plaintiff incorporates paragraphs 1-32 as if fully set forth herein.

97. Plaintiff and the Class members delivered and entrusted their private information to Defendants for the sole purpose of receiving services from Defendants.

98. During the time of bailment, Defendants owed Plaintiff and Class members a duty to safeguard this information properly and maintain reasonable security procedures and practices to protect such information. Defendants breached this duty.

99. As a result of this breach of duty, Plaintiff and Class members have suffered harm.

COUNT VI
Unjust Enrichment
(On Behalf of Plaintiff and the National Class)

100. Plaintiff incorporates paragraphs 1-32 as if fully set forth herein.

101. Plaintiff brings this Count in the alternative to Count II to the extent that an implied contract is not found to exist between Defendants and Plaintiff and the members of the Class, in which case Plaintiff and the members of the Class will have exhausted all other remedies against Defendants.

102. Defendants received payment from Plaintiff and Class members to perform services that included protecting Plaintiff's and Class members' private personal and financial information.

103. Defendants did not protect Plaintiff's and the Class members' information, but retained Plaintiff's and Class members' payments.

104. Defendants retained the benefits of Plaintiff's and Class members' payments under circumstances which rendered it inequitable and unjust for Defendants to retain such benefits without paying for their value.

105. Defendants have knowledge of said benefits.

106. Plaintiff and the members of the Class are entitled to recover damages in an amount to be proven at trial.

VII. DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury of all claims in this complaint so triable.

VIII. REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Class proposed in this Complaint, respectfully requests that the Court enter judgment in his favor and against Defendants as follows:

A. Declaring that this action is a proper class action, certifying the Class as requested herein, designating Plaintiff as Class Representative and appointing the undersigned counsel as Class Counsel for the Class;

B. Ordering Defendants to pay monetary damages to Plaintiff and the other members of the Class;

C. Ordering Defendants to pay for not less than three years of credit card monitoring services for Plaintiff and the other members of the Class;

D. Ordering Defendants to pay punitive damages, as allowable by law, to Plaintiff and the other members of the Class;

E. Ordering Defendants to pay statutory damages, as provided by the Illinois Consumer Fraud and Deceptive Business Practices Act and other applicable State Consumer Fraud Acts, to Plaintiff and the other members of the Class;

F. Ordering Defendants to disseminate individualized notice of the Security Breach to all Class members and to post notice of the Security Breach on their website(s);

G. Ordering Defendants to pay attorneys' fees and litigation costs to Plaintiff and the other members of the Class;

H. Ordering Defendants to pay both pre- and post-judgment interest on any amounts awarded; and

I. Ordering such other and further relief as may be just and proper.

Dated: September 2, 2015

Respectfully submitted,

JOHN DOE, individually and on behalf of all others similarly situated

/s/Joseph J. Siprut
Joseph J. Siprut
jsiprut@siprut.com
Michael L. Silverman
msilverman@siprut.com
SIPRUT PC
17 N. State Street
Suite 1600
Chicago, Illinois 60602
Phone: 312.236.0000

Katrina Carroll
kcarroll@litedepalma.com
Kyle A. Shamberg
kshamberg@litedepalma.com
LITE DEPALMA GREENBERG, LLC
211 W. Wacker Drive
Suite 500
Chicago, Illinois 60606
Phone: 312.750.1591

Robert Ahdoot
rahdoot@ahdootwolfson.com
Tina Wolfson
twolfson@ahdootwolfson.com
AHDOOT & WOLFSON, PC
1016 Palm Avenue
West Hollywood, California 90069
Phone: 310.474.9111